Amendments to the Claims

Replace all prior versions and listings of claims in the application with the following list of claims.

1. (**currently amended**) A digital computing apparatus capable of detecting and preventing a plurality of rate based and non rate based denial of service attacks, said apparatus comprising:

a media access controller (MAC) interface **connected to an unprotected side of a network and to a protected side of the network**;

a classification means operatively coupled to said MAC interface for classifying data packets received from **the unprotected side of the network through** said MAC interface according to Layer 2, Layer 3, and Layer 4 classifications, said classification means being capable of enforcing Layer 2, Layer 3, and Layer 4 accepted header syntax**, wherein the classifying comprises isolating header values and performing hierarchical protocol classification**;

a meter means operatively coupled to said classification means, said meter means having a plurality of meters and being capable of maintaining statistics of said attacks and determining whether a threshold has been reached;

a decision multiplexer means operatively coupled to said meter means, said decision multiplexer means being capable of accepting decisions from said plurality of meters and informing a single decision to said MAC interface;

an ager means capable of timing out flood states identified by said classification means or by said meter means, said ager means comprising a continuous learning mechanism for continuously learning and updating said statistics;

a source tracking mechanism multiplicatively incrementing count for sources that send identified flood data, thereby distinguishing said sources from others that send non-flood data;

a SYN flood detection and prevention mechanism having a support means for creating a plurality of legitimate IP addresses during normal operation when ~~the~~ **a** TCP state **of TCP connections through the MAC interface** transitions to ESTABLISHED, wherein said SYN flood detection and prevention mechanism allows only said plurality of legitimate IP

addresses to be stored during normal operation, **wherein the TCP state of the TCP connections is maintained by a TCP state machine in the apparatus**;

and

a zombie flood detection and prevention mechanism having

a means for limiting connections **from the MAC interface** to said plurality of legitimate IP addresses stored during normal operation; and

a means for determining a threshold for said connections based on baseline traffic learned during normal operation;

wherein said support means for creating said plurality of legitimate IP addresses adds an IP address to said plurality of legitimate IP addresses when the TCP state **of the TCP connections through the MAC interface** transitions to "established" for the first time;

wherein said plurality of legitimate IP addresses comprises IP addresses which have established valid TCP connections **through the MAC interface**.

2. (**original**) The apparatus of claim 1, wherein said plurality of meters detect and prevent rate based denial of service attacks selected from the group consisting of synchronization (SYN) flood, Transmission Control Protocol (TCP) flood, Internet Control and Message Protocol (ICMP) flood, User Datagram Protocol (UDP) flood, port scan, source flood, destination flood, broadcast flood, Address Resolution Protocol (ARP) flood, Reverse ARP (RARP) flood, multicast flood, Virtual Local Area Network (VLAN) flood, double encapsulated VLAN flood, protocol flood, Internet Protocol (IP) option flood, fragment flood, port flood, Layer 2 floods, Layer 3 floods, and Layer 4 floods.

3. (**original**) The apparatus of claim 2, wherein said rate based denial of service attacks are to an end node or from said end node to other nodes on the internet.

Claims 4-7. (**cancelled**).

8. (**original**) The apparatus of claim 1, wherein said ager means monitors said statistics maintained by said plurality of meters.

9. (**original**) The apparatus of claim 8, wherein said plurality of meters identify whether a threshold of counts has been reached for a flood state corresponding to a packet header value.

10. (**original**) The apparatus of claim 9, wherein said plurality of meters inform said decision multiplexer means to block traffic with said packet header value.

Claims 11-20 (**cancelled**).

21. (**currently amended**) A computer-implemented method for rate-based denial of service attack detection **implemented at an apparatus positioned between a protected side of a network and an unprotected side of the network**, the method comprising:

receiving packets from **the unprotected side of the** ~~a~~ network;

classifying the received packets according to network layer 2, 3, 4 classification**, wherein the classifying comprises isolating header values and performing hierarchical protocol classification**;

metering the classification to produce statistics related to multiple types of attacks;

creating and storing a table of legitimate IP addresses during normal operation when a TCP state **of TCP connections through the apparatus** transitions to "established";

detecting a SYN flood state;

dropping **at the apparatus** packets from IP addresses not in the table of legitimate IP addresses during the detected SYN flood state;

detecting a zombie flood state when a number of packets **received at the apparatus** from legitimate IP addresses exceeds a threshold; and

dropping **at the apparatus** packets from IP addresses in the table of legitimate IP addresses during the detected zombie flood state;

wherein creating and storing the table of legitimate IP addresses comprises:

adding an IP address to the table of legitimate IP addresses when the TCP state **of TCP connections through the apparatus** transitions to "established" for the first time; and

maintaining in the table of legitimate IP addresses a list of IP addresses which have established valid TCP connections **through the apparatus**.